AO 93 (Rev. 12/09) Search and Seizure Warrant (USAO CDCA Rev. 01/2013)

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)	
One Western Digital hard drive with serial number WCAL92444808 taken from a generic desktop computer with no serial number ("SUBJECT ITEM #1")	)	Case No. M 15 00007

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A(1).

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property. Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 01-05-2015 2:30 pm

Judge's signature

City and state: Los Angeles, California

The Hon. Stephen J. Hillman, U.S. Magistrate Judge
Printed name and title

AUSA: Lindsey Greer Dotson

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.:	*Date and time warrant executed:*	*Copy of warrant and inventory left with:*
M 15 00007	1/7/15 1:15 PM	Patricia Shannon

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]

One Western Digital hard drive with serial number WCAL92444808

Certification (by officer present during the execution of the warrant)

I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: 1/12/2015

Executing officer's signature

Kelly Nowak Special Agent

Printed name and title

AUSA: Lindsey Greer Dotson

ATTACHMENT A(1)

ITEM TO BE SEARCHED

The item to be searched is a digital device seized from 3416 W. Orange Avenue, Apt. 205, Anaheim, California 92804 and currently located at HSI facilities in Long Beach, California, specifically the following of the SUBJECT ITEMS described in the attached affidavit: One Western Digital hard drive with serial number WCAL92444808 taken from a generic desktop computer with no serial number ("SUBJECT ITEM #1").

ATTACHMENT B

ITEMS TO BE SEIZED

The SUBJECT ITEMS described in Attachments A(1), A(2), and A(3) themselves constitute instrumentalities of violations of Title 18, United States Code, Sections 2252A (a)(5)(B), (b)(2) (Possession of Child Pornography) and therefore should be seized.

In addition, the following are items to be seized from the SUBJECT ITEMS, which I believe constitute the fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252A (a)(5)(B), (b)(2) (Possession of Child Pornography):

1. Items to be seized:

a. Child pornography, as defined in Title 18, United States Code, Section 2256(8).

b. Records, documents, programs, applications, or materials, or evidence of the absence of same, sufficient to show ownership of and the actual users of the SUBJECT ITEMS.

c. Records, documents, or materials pertaining to the possession of child pornography.

d. Correspondence establishing possession, access to, or transmission through interstate or foreign commerce, of child pornography or identifying any minor visually depicted while involved in sexually explicit conduct.

e. Records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce of child pornography.

f. Any items that are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct, including written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

g. Any programs or records that pertain to peer-to-peer file sharing software.

h. Financial documents, including, but not limited to, bank statements and credit card information that may relate to or contain evidence of the above-referenced offenses.

i. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show Internet access, search, and use history contained in the SUBJECT ITEMS.

2. As used both above and below, the term "digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including an external hard drive.

3. In searching the SUBJECT ITEMS and in searching digital data stored on the SUBJECT ITEMS, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel, including but not limited to certified forensic analyst Bruce W. Pixley of the Pixley Forensics Group, will, in their discretion, either search the digital device on-site or seize and transport the device to an appropriate law enforcement laboratory or similar facility to be searched at that location. The team of law enforcement personnel, which may include the investigating agents and/or individuals assisting law enforcement personnel searching the SUBJECT ITEMS, shall complete the search as soon as is practicable but not to exceed 60 days from the date of the issuance of this warrant. If additional time is needed, the Government may seek an extension of this time period from the Court within the original 60-day period from the date of execution of the warrant.

b. The team searching the SUBJECT ITEMS will do so only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The team may subject all of the data contained in the SUBJECT ITEMS capable of containing items to be seized as specified in this warrant to the protocols to determine whether the SUBJECT ITEMS and any data falls within the items to be seized as set forth herein. The team searching

the SUBJECT ITEMS may also search for and attempt to recover "deleted," "hidden," or encrypted data to determine, pursuant to the protocols, whether the data falls within the list of items to be seized as set forth herein.

ii. The team searching the SUBJECT ITEMS also may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The team may use EnCase or another similar program to identify child pornography.

c. When searching the SUBJECT ITEMS pursuant to the specific protocols selected, the team searching the SUBJECT ITEMS shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the team searching the SUBJECT ITEMS pursuant to the selected protocols encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that SUBJECT ITEMS pending further order of Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. At the conclusion of the search of the digital devices as set forth in subparagraph (a) above, all the data on the SUBJECT ITEMS shall be retained by the Government until further order of the Court or one year after the conclusion of the criminal case.

f. Notwithstanding the above, after the completion of the search of the SUBJECT ITEMS as set forth in subparagraph (a) above, the Government shall not access digital data falling outside the scope of the items to be seized in this warrant on any retained SUBJECT ITEMS or digital data absent further order of the Court.

4. The special procedures relating to digital media found in this warrant govern only the search of digital media pursuant to the authority conferred by this warrant and do not apply to any search of digital media pursuant to any other court order.

EXHIBIT 1

AGENT

AFFIDAVIT FOR SEARCH WARRANT

COPY

UNITED STATES DISTRICT COURT	CENTRAL DISTRICT OF CALIFORNIA
UNITED STATES OF AMERICA VS. THE PROPERTY KNOWN AS: 3416 W. Orange Ave. Apt. #205W Anaheim, California 92804	DOCKET NO. MAGISTRATE CASE NO. SA09-336M NAME AND ADDRESS OF JUDGE OR U.S. MAGISTRATE JUDGE ROBERT N. BLOCK UNITED STATES MAGISTRATE JUDGE SANTA ANA, CALIFORNIA

The undersigned being duly sworn deposes and says: That there is reason to believe that

☒ in the property known as	DISTRICT CENTRAL DISTRICT OF CALIFORNIA

See Attachment "A"

FILED
CLERK, U.S. DISTRICT COURT
JUL 22 2009
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

The following items are concealed:

See Attachments "B"

FILED
CLERK, U.S. DISTRICT COURT
2009 JUL 22 AM 10:33
CENTRAL DISTRICT OF CALIFORNIA
BY

Affiant alleges the following grounds for search and seizure [1]

The items to be searched for constitute evidence of violations of the following sections: Title 18, United States Code, Sections 2252A(a) (2), 2252A(a) (3) (B), 2252A(a) (5) (B)

Affiant states the following facts establishing the foregoing grounds for issuance of a Search Warrant

(SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED AS PART OF THIS AFFIDAVIT FOR SEARCH WARRANT)

SIGNATURE OF AFFIANT:	Araceli Trevino SPECIAL AGENT, IMMIGRATION AND CUSTOMS ENFORCEMENT

Sworn to before me, and subscribed in my presence:

DATE:	JUDGE, [2] OR US MAGISTRATE JUDGE ROBERT N. BLOCK
July 22, 2009	ROBERT N. BLOCK

[1] If a search is to be authorized "at any time in the day or night" pursuant to Federal Rules of Criminal Procedure 41(c), show reasonable cause therefor
[2] United States Judge or Judge of a State Court of Record

AG:fgs
AG

AFFIDAVIT

I, Araceli Trevino, being duly sworn, depose and state the following:

I. INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), assigned to the Office of the Assistant Special Agent in Charge, Orange County, California. I have been so employed since February 2002. As part of my duties as an ICE agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography[1] in all forms of media including computer storage media. I have also authored search warrant affidavits and participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography offenses.

2. The information contained in this Affidavit is based

[1] The term "child pornography," as used in this affidavit, is defined as set forth in 18 U.S.C. § 2256(8)(A) and (8)(C).

upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and the review of documents and records.

II. PURPOSE OF AFFIDAVIT

3. The purpose of this application is to search for and seize evidence of violations of Title 18, United States Code, Sections 2252A(a)(2) (receipt and distribution of child pornography), 2252A(a)(3)(B) (advertisement of child pornography) and 2252A(a)(5)(B) (possession of child pornography), specifically those items listed in Attachment B, below.

4. The statements contained in this affidavit are based upon my training and experience, information provided to me by other law enforcement officers and witnesses as part of this investigation. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have only set forth facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2252A(a)(2) (receipt and distribution of child pornography), 2252A(a)(3)(B) (advertisement of child pornography), and 2252A(a)(5)(B) (possession of child pornography) is presently located at the "SUBJECT PREMISES."

III. PREMISES TO BE SEARCHED

5. This affidavit is made in support of an application for a warrant to search the entire premises located at 3416 W. Orange Ave. Apt #205W, Anaheim, CA 92804. The "SUBJECT PREMISES" is more particularly described as follows: A two-story multiple-unit apartment complex has a peach stucco exterior color, brown and white wood fascia boards and bears a brown composition roof. The front of the complex faces north and the building numbers posted is "3416," which are white in color. The "SUBJECT PREMISES" is on the second floor and the front door faces west. The front door is wooden and white in color, has a white wrought iron security door, and a blue wrought iron staircase that leads to the "SUBJECT PREMISES." On the middle of the door black metallic numbers "205" is affixed to the exterior part of the white wooden door. West of the front door is a window with white vertical blinds, which faces south. Adjacent to the front door a light fixture is affixed to the wall and faces south.

IV. SUMMARY

6. As set forth in detail below, there is probable cause to believe that Adrian C. CAZACU at the "SUBEJCT PREMISES," purchased at least one subscription to an Internet website that was distributing child pornography.

V. COMPUTERS, THE INTERNET, AND CHILD PORNOGRAPHY

7. As part of my training, I have become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail"). An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet - for example, through a university, an employer, or a commercial service - which is called an "Internet Service Provider" or "ISP" (see definition of "Internet Service Provider" below). Once the individual has accessed the Internet, that individual can use Internet mail services, including sending and receiving e-mail. In addition, the individual can visit websites (see

definition of "websites" below), and make purchases from them or otherwise communicate with the operators of the website.

8. Set forth below are some definitions of technical terms, most of which are used throughout this Affidavit pertaining to the Internet and computers more generally.

a. **Client/Server Computing:** Computers on the Internet are identified by the type of function they perform. A computer that provides resources for other computers on the Internet is known as a **server**. Servers are known by the types of service they provide, that is, how they are configured. For example, a **web server** is a machine that is configured to provide web pages to other computers requesting them. An **e-mail server** is a computer that is configured to send and receive electronic mail from other computers on the Internet. A **client computer** is a computer on the Internet that is configured to request information from a server configured to perform a particular function. For example, if a computer is configured to browse web pages and has web page browsing software installed, it is considered a **web client**.

b. **Domain Name:** Domain names are common, easy to remember names associated with an Internet Protocol address (defined below). For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain

names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards - from right to left - further identifies parts of an organization. Examples of first level, or top-level domains are typically .com for commercial organizations, .gov for the United States government, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

When a user types in the domain name of a website he or she wants to view in an Internet browser, a request is sent from the user's computer to the server that is hosting that website. This server is found via the Domain Name Server system, which associates the domain name, in the above example, www.usdoj.gov, and the Internet Protocol address of the server that is hosting that website, in the above example, 149.101.1.32. Once that request is received by the server, the server provides a "response," and completes the basic cycle that makes websites

work: the browser makes a request, the server processes that request, including accessing any images, and returns the appropriate response to the browser. When all the files that are required to display a webpage have been downloaded, including all images, the browser is then able to properly display the website. The process then starts all over again if a link located on the website is clicked, which triggers the browser to make a request for another file from the server.

c. **Internet Service Providers ("ISPs") and the Storage of ISP Records:** Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name - a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password

selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use.

d. **Internet Protocol ("IP") Address**: Typically, computers or devices on the Internet are referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is

assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next dial-up customer. On the other hand, some ISPs, including some cable providers, employ static IP addressing, that is, a customer or subscriber's computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer.

e. **Log File:** Log files are records automatically produced by computer programs to document electronic events that

occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

f. **Modem**: A modem is an electronic device that allows one computer to communicate with another.

g. **Website**: A website consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

h. **Uniform Resource Locator ("URL")**: A URL is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in an Internet browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that

identifies the specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

i. **Website Hosting:** Website hosting provides the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a website, the client needs a server and perhaps a web hosting company to host it. **"Managed hosting"** means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. **"Co-location"** means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house their hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

9. Based upon my knowledge, training, and experience in investigating child exploitation and child pornography cases,

and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership-based/subscription-based websites to conduct business, allowing them to remain relatively anonymous.

10. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law

enforcement officers with whom I have had discussions, I know that the development of computers has also revolutionized the way in which those who seek out child pornography are able to obtain this material. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by those who seek to obtain access to child pornography in these ways:

a. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for

law enforcement to follow.

b. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as America Online ("AOL") and Microsoft, which allow subscribers to dial a local number and connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

c. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next

door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache[2] to look for "footprints" of the websites and images accessed by the recipient.

d. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a "hard drive") used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 160 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a

---

[2] "Cache" refers to text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website.

video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

VI. BACKGROUND INVESTIGATION[3]

A. Overview of Operation Emissary, Phase One

11. On or about January 12, 2009, I obtained reports/documents from Special Agent ("SA") Patrick Lee, assigned to the Office of the Special Agent in Charge, Los Angeles, California. The ICE investigation which has generated the evidence demonstrating that there is probable cause to search the "SUBJECT PREMISES" is known as Operation Thin Ice. Operation Thin Ice represents the third phase of Operation Emissary, an investigation into the operators of and subscribers to hard-core child pornography websites available worldwide over the Internet. Operation Emissary began in late 2005 and, to date, has resulted in more than 300 domestic convictions of subscribers to those websites. Those convictions, which span

[3] The information set forth in this section is provided as a broad overview of the investigation conducted to date. It does not include a listing of all investigative techniques employed or even the full and complete results of any of the listed investigative efforts.

approximately 40 states, include dozens of convicted sex offenders and child molesters. A brief description of the first two phases of Operation Emissary and Operation Thin Ice follows.

12. On or about October 2005, ICE agents in New Jersey located a hard-core child pornography website available on the Internet that advertised access to images and videos of child pornography via the Internet. This Child Pornography Advertising Website[4] allowed a person seeking such access to pay

---

[4] This particular website labeled itself "Illegal.CP." Through further investigation, and as explained below in the discussion of Operation Thin Ice, the individuals operating the Illegal.CP website operated a two-tier system of child pornography websites. The first tier consisted of a group of websites (the "Child Pornography Advertising Websites"), like the Illegal.CP website, that displayed sample images of child pornography and that advertised and provided a means to purchase access to the second tier, a website containing thousands of hard-core images and videos of child pornography (the "Child Pornography Website"). Throughout this Affidavit, the operators of the two tiers, who have remained constant throughout this investigation, will be referred to as the "Operators of the Child Pornography Website."

The Child Pornography Advertising Websites included, but were not limited to, websites labeling themselves "The Sick Child Room," "Hottest Childporn Garden," "Real Child Porno," "Children Porno," "CP City 2007," "Pedo Heaven," "Dirty Nymphets," "World Famous Childporn Video" and "Hottest Childporn Garden." For the purposes of this Affidavit, a first tier website will be referred to as a "Child Pornography Advertising Website," unless otherwise noted. Over the past three to four years, the Operators of the Child Pornography Website have moved the server on which the contents of the Child Pornography Website are stored on a regular basis, undoubtedly to avoid detection and any disruption in service to subscribers, often with a new URL being employed for each new server. These URLs have included, but were not limited to, http://hualama.cjb.net/

a $79.99 fee via credit card. To purchase such access, an individual had to enter his personal and credit card information into the "join page" of the Child Pornography Advertising Website. The "join page" was a webpage that contained fields in which a purchaser entered his personal and credit card information to consummate the purchase, including, among other things, his name, address, e-mail address, and credit card number, "cvv,"[5] and expiration date. There were also fields for the purchaser to enter a proposed login and password.

13. On or about October 26, 2005, an ICE agent ("UC-1") made an undercover purchase through the Child Pornography

---

and http://www.ciampics.com.

The contents of the Child Pornography Website has changed over time as well, generally with the addition or removal of particular images or videos of child pornography. Technically, the Child Pornography Website may therefore be described as a series of very similar websites containing thousands of images and videos of child pornography used over time by the Operators of the Child Pornography Website as part of their scheme. As set forth in paragraph 53 below, I have reviewed the contents of the Child Pornography Website as it appeared when the search warrants were conducted on Hivelocity. I found child pornography and child erotica. Three typical images and/or videos are described in more detail in paragraph 56, below. Although I did not view every single image on this website, I saw exclusively child pornography and child erotica.

[5] A credit card's "cvv" is a security identification number often found on the back of a credit card. Merchants often require credit card users to disclose their credit cards' cvvs to help verify that the users are in possession of the actual credit card.

Advertising Website. UC-1 entered information into all of the fields on the "join page" of that Child Pornography Advertising Website using an undercover identity, including an undercover e-mail address (the "UC-1 E-mail Account") and undercover credit card information.

14. On or about October 27, 2005, an e-mail from theodore_dykstra@hotmail.com (the "Dykstra E-mail Account") was received at the UC-1 E-mail Account. The e-mail contained the login and password that UC-1 had entered on the "join page" of the Child Pornography Advertising Website on or about October 26, 2005, and included instructions to visit the Child Pornography Website. The e-mail message also stated that the credit card would be charged by "ADSOFT" for the purchase price of $79.99.

15. When the credit card statement for the undercover credit card used for the October 26, 2005 purchase made through the Child Pornography Advertising Website was received, it reflected a charge of $79.99 to "AD SOFT."[6]

16. Subsequent to receiving that e-mail, UC-1 accessed the Child Pornography Website listed in the October 27, 2005 e-mail

---

[6] Through subsequent investigation, ICE agents determined that "AD SOFT" was a sham merchant set up by the Operators of the Child Pornography Website to disguise the nature of the credit card purchases of access to child pornography. The website for AD SOFT purported to sell computer software, including "anti-spyware," but, in fact, no such products could be purchased through that website.

from the Dykstra E-mail Account. Upon accessing the Child Pornography Website, UC-1 was brought to a webpage that contained fields in which to enter a login and password.

17. Upon entering the login and password provided by the October 27, 2005 e-mail described above, UC-1 was redirected to another webpage at the top of which appeared the following:

> FAQ, Please read. "Our site is considered to be illegal in all countries.... Even if you ever have problems with police, you can always say that someone had stolen the information from your credit card and used it. It is very difficult to establish that you were the person to pay."[7]

18. At the bottom of that webpage was a link titled "Continue." Upon clicking on that link, UC-1 was taken to a webpage that made available thousands of images of child pornography.

19. Subsequently, ICE agents were able to determine that the contents of the Child Pornography Website were being housed on a server in Orlando, Florida. Pursuant to a court-authorized search warrant, agents conducted a search of this server in or about mid-November of 2005 and recovered thousands of images and videos of child pornography which the Operators of the Child Pornography Website stored on that server. Further, a review of

---

[7] All misspellings and grammatical errors contained within the block quote are the errors of the original authors.

the contents of the server revealed log files containing IP addresses associated with all contacts to the Child Pornography Website, which had occurred during a period of approximately nine days during mid-November 2005. Specifically, this data revealed that hundreds of IP addresses presumably associated with individual subscribers who had visited the Child Pornography Website during this nine-day period. The data also demonstrated which individual child pornography images had been accessed by each IP address. Two additional search warrants were executed on the Orlando, Florida server on or about December 14, 2005 and January 5, 2006. Both searches produced additional log files documenting contacts from specific IP addresses with particular images available through the Child Pornography Website. During November and December 2005, it is believed that the Operators of the Child Pornography Website shifted the location of the images and videos of child pornography to a different server and began phasing out the use of the Orlando, Florida server.

20. On or about December 23, 2005, the Honorable William J. Martini, United States District Judge for the District of New Jersey, signed an order authorizing the interception of electronic communications occurring over the Dykstra E-mail Account. Actual interception pursuant to that order commenced

on December 27, 2005. Over the following thirty day period, numerous e-mail communications were intercepted pertaining to individuals attempting to purchase access to images and videos of child pornography accessible through the Child Pornography Website. Based on those interceptions, ICE agents were able to determine the following:

a. The Operators of the Child Pornography Website controlling the Dykstra E-mail Account received the information submitted by an individual attempting to purchase a subscription to images and videos of child pornography by some means or pathway other than the Dykstra E-mail Account. That information included, among other things, the name of the subscriber, the subscriber's address, the subscriber's credit card information and the subscriber's e-mail address.

b. The Operators of the Child Pornography Website controlling the Dykstra E-mail Account then typically transmitted this information via an attachment to an e-mail to one of several e-mail addresses, including admin@ad-soft.net. The Dykstra E-mail Account then received a return e-mail, typically on the same day, from one of the previously referenced e-mail accounts which effectively advised whether the individual should be accepted or rejected as a subscriber or whether some other action should be taken based on a verification process related to the credit card number submitted.

c. Finally, an e-mail from the Dykstra E-mail Account was sent to the individuals whose credit card information has been satisfactorily verified (a) informing them that their purchase had been approved; (b) providing a password and login (typically those which have been previously selected by the would-be subscriber) to access the images and videos of child pornography; and (c) supplying at least one URL to the Child Pornography Website through which to access the

images and videos of child pornography.[8]

21. Interception of electronic communications over the Dykstra E-mail Account ended pursuant to the December 23, 2005 order on January 25, 2006. Pursuant to an order signed by the Honorable William J. Martini authorizing continued interception of electronic communications over the Dykstra E-mail Account, interception resumed on or about January 27, 2006 and continued through February 25, 2006. During this time period, the operator of the Dykstra E-mail Account granted access to the images and videos of child pornography to hundreds of individual purchasers.

22. During the period of authorized interception, ICE agents determined that the Operators of the Child Pornography Website had shifted the images and videos of child pornography to a new server located in McLean, Virginia, which began hosting that content from as early as December 2005. In or about February and March of 2006, searches of this Virginia-based server were conducted pursuant to court-authorized search warrants. Those searches revealed the presence of thousands of images and videos of child pornography accessible on the server

[8] Agents determined that the e-mail message notifying individual subscribers that their purchase had been approved and would be billed by ADSOFT was not always sent via the Dykstra E-mail Account, but from other e-mail accounts as well.

through the Child Pornography Website. In addition, numerous log files ranging from the period from October of 2005 through early February 2006 were obtained which documented contact by numerous IP addresses. These log files also included a variety of data of individuals who had purchased subscriptions, including a subscriber's ID, a subscriber's login, the subscriber's e-mail address and the date and time when the subscription began and the IP address from which the images and videos of child pornography were accessed.

23. Based on the evidence gathered via the interception of e-mail communications over the Dykstra E-mail Account and the log files retrieved from the servers in Florida and Virginia, ICE agents were able to identify hundreds of individuals in the United States who had successfully purchased child pornography subscriptions to the Child Pornography Website from in or about November 2005 through in or about February 2006. These leads were disseminated to ICE offices across the country during mid-2006, and agents began executing search warrants in approximately August 2006. As a result of the execution of numerous search warrants from in or about August through in or about October 2006, ICE was able to announce the arrest of more than 125 individuals in or about late October 2006. ICE agents executed additional search warrants through late 2006 and early

2007.[9] In total, the first phase of Operation Emissary has resulted in more than 250 convictions, primarily in federal court, in over 36 states.

B. Operation Emissary, Phase Two

24. With the disbursement of the Phase I leads to ICE offices across the United States, ICE agents in the District of New Jersey began to focus upon the flow of the money generated by the credit card purchases of individual child pornography subscribers. The financial investigation led to the identification of hundreds of additional subscribers during the period from late February 2006 through mid-July 2006.

25. Specifically, agents were able to determine that credit card transactions for the purchases of access to the images and videos of child pornography described in the previous paragraphs were being processed through a credit card processing

[9] The execution of search warrants in both Phases I and II of Operation Emissary produced an exceptionally high success rate in terms of uncovering evidence of the commission of child pornography offenses. Approximately 90 percent of those search warrants led to the recovery of images of child pornography and/or admissions by individuals that they had attempted to access child pornography. For example, in the District of New Jersey, ICE agents executed approximately 22 search warrants during Phases I and II of Operation Emissary. Images and/or videos of child pornography were recovered as a result of 19 of the 22 search warrants. Of the three remaining search warrants, two of the three targets confessed to obtaining a subscription to child pornography websites and subsequently pled guilty in federal court.

company known as JetPay based in Carrollton, Texas. In approximately mid-September 2006, ICE agents executed a court-authorized search warrant at the offices of JetPay in Texas. This search resulted in the retrieval of a database listing the credit card numbers and associated data which had been submitted by individuals attempting to purchase such access during the period from February 2006 through mid-July 2006. The data retrieved included, among other things, the following which had been submitted by each individual attempting to purchase such access: name, credit card number and address, including street address, city, country and zip code. In addition, the database recorded the price of the purchase, the date and time that the transaction had been processed, and the company under which the transaction would be billed, i.e. "AD SOFT."

26. During January 2007, ICE dispersed the leads recovered from the JetPay database to ICE offices throughout the country. To date, numerous search warrants and consent searches have been executed based on those leads, and more than 50 individuals have been convicted nationwide as of November 2008.

C. Operation Emissary, Phase Three: Operation Thin Ice

1. The Cooperating Witness

27. During the course of Phases I and II of Operation Emissary, ICE agents were able, through the use of numerous

investigative techniques, to identify an individual involved in processing the credit card transactions for the Child Pornography Website (the Cooperating Witness, or "CW").

28. The CW was arrested by ICE agents in or about March 2008, and charged with a violation of 18 U.S.C. § 1956(h), conspiracy to launder monetary instruments, because of the CW's role in processing those credit card transactions. The CW has since pleaded guilty to a violation of 18 U.S.C. § 1956(h) and has entered into a cooperation agreement with the Government. During CW's guilty plea, the CW admitted to processing the credit card transactions associated with the sale of access to images and videos of child pornography via the Internet, a reference to the sale of subscriptions to child pornography through the Child Pornography Advertising Websites.

29. The CW has cooperated with ICE agents in their investigation of the Operators of the Child Pornography Website. The CW informed ICE agents of the following:

a. The CW's role was to process the credit cards used by purchasers of access to the images and videos of child pornography available through the Child Pornography Website.

b. After an individual entered his personal information, including his name, address, and credit card information into the "join page" of a Child Pornography

Advertising Website, that information was then transmitted via the Internet to one of the Operators of the Child Pornography Website. That Operator of the Child Pornography Website would then send the information to the CW, who had retained a credit card processing company to process the online credit card transactions through a merchant account established by the CW.

c. If the transaction was approved, the CW would then receive the amount of the purchase from the bank that issued the purchaser's credit card, and that charge would subsequently appear on the purchaser's credit card statement. The CW would then transfer those proceeds, minus various fees and the CW's percentage, to the Operators of the Child Pornography Website.

d. To disguise the nature of the transaction, a purchase made through a Child Pornography Advertising Website would appear on a purchaser's credit card statement as a purchase of legitimate goods or services from a sham merchant created by the CW, such as AD SOFT. According to the CW, AD SOFT has never been associated with or sold any legitimate product. The CW stated that AD SOFT was solely used as a billing descriptor for credit card purchases of access to images and videos of child pornography. The CW explained that the CW had used a number of sham Internet-based companies to process

such credit card transactions, including AD SOFT, which purported to offer items for sale ranging from weight-loss products to computer anti-spyware software.

30. Because most of the CW's prior communications with the Operators of the Child Pornography Website were via the Internet, the CW had limited information regarding their full identities.[10] The CW's cooperation was therefore initially directed, first and foremost, to obtaining information regarding the full identities of the Operators of the Child Pornography Website. During one communication between the CW and one of the Operators of the Child Pornography Website, the CW was informed that the Operators of the Child Pornography Website were in the process of establishing a United Kingdom-based merchant account through another individual to process credit card transactions for child pornography purchases, with that individual taking a 50 percent cut from such transactions.

31. Under the direction and supervision of ICE agents, the CW contacted the Operators of the Child Pornography Website via ICQ, an internet-based instant messaging service. The CW represented to the Operators of the Child Pornography Website

---

[10] The CW had met one of the Operators of the Child Pornography Website in person. The CW did not, however, have information regarding the full identity of that operator, such as the operator's full name, exact location, and other identifying information.

that the CW had a partner who could obtain a United States-based merchant account from a third-party credit card processor to process credit card transactions for individuals seeking to purchase access to images and videos of child pornography via the Internet.[11] The CW also represented that the CW would take a 10 percent cut from such transactions, in addition to any costs associated with processing, and that the CW's partner would take a 20 percent cut.

32. In or about March 2008, the Operators of the Child Pornography Website agreed to have the CW process credit card transactions for access to images and videos of child pornography that they made available via the Internet. The billing descriptor for the CW's merchant account was "NEWSAC." As part of its investigation, ICE agents set up another undercover e-mail account (the "CW E-mail Account"), which the agents monitored and controlled. The CW provided the CW E-mail Account to the Operators of the Child Pornography Website so that they could send to the CW the personal and credit card information that had been captured when individuals entered that information into the "join page" of a Child Pornography Advertising Website.

---

[11] According to the CW, United States-based merchant accounts are generally preferred because the payouts to the merchants are made more frequently than for overseas accounts.

33. After the NEWSAC merchant account became operational, the Operators of the Child Pornography Website began to forward to the CW E-mail Account lists of individuals attempting to purchase access to images and videos of child pornography through one of the Child Pornography Advertising Websites. Those e-mails were sent from the e-mail address "nolimitzory@aim.com."

34. The format of the lists of subscribers sent to the CW E-mail Account was essentially unchanged from that which had been intercepted over the Dykstra E-mail Account during Phase I of Operation Emissary. Among the data included in this list were the following items, among other things, submitted by the would-be subscriber: name, address, e-mail account, password and login selected, and credit card number with expiration date. Also included were the IP address from which the purchase was made and the URL of the Child Pornography Advertising Website "join page" through which the purchase was made. This information revealed that the Operators of the Child Pornography Website used several Child Pornography Advertising Websites to sell access to child pornography on the Internet. These Child Pornography Advertising Websites generally had the same basic structure, including a "join page" in which a purchaser entered credit card and personal information to effect the purchase.

35. The credit cards were then processed through the NEWSAC merchant account. If the credit card was processed successfully, a number would be generated indicating that the payment would be processed and the credit card charged. If the credit card was not processed successfully, the merchant account would indicate that payment had been declined. After the individual credit cards on the daily subscriber list had been run through the NEWSAC merchant account, an e-mail was sent from the CW E-mail Account to nolimitzory@aim.com indicating which of the credit cards had been processed successfully and for which payment had been declined. This e-mail would list all of the would-be subscribers by their e-mail addresses.[12]

2. **The 2008 ICE Undercover Purchase**

36. During the first two phases of Operation Emissary, ICE agents used an undercover email account to purchase access to hard-core child pornography websites (the "ICE Undercover E-mail Account"). In or about March 2008, shortly after the Operators of the Child Pornography Website agreed to have the CW process credit card transactions for the sale of child pornography, ICE agents received an e-mail at the ICE Undercover E-mail Account.

[12] This format followed the same pattern which had been employed by the CW for years and which had been intercepted on a daily basis over the Dykstra E-mail Account during Phase I of Operation Emissary.

The e-mail had the subject line heading of "MEET LITTLE KIDS ONLINE VIDEO."[13] This e-mail informed the recipient that "[w]e issued a new collection of true C.H.1/L/D P/O.R.N.," and advertised "[v]ery little kids, new exclusive photo and video archives, hard scenes." The e-mail also encouraged the recipient to "[c]heck our preview page at: http://www/sesoqaj.com/lua."[14]

37. On or about March 25, 2008, ICE agents accessed the URL listed in the e-mail described in the previous paragraph, which brought the agents to a Child Pornography Advertising Website labeling itself "Pedo Heaven" (the "Pedo Heaven Website") which proclaimed that it was "Simply the best PTHC[15] place in the entire WORLD!" The Pedo Heaven Website advertised access to images and videos of child pornography images on the internet for a period of thirty days for a payment of $79.99. The Pedo Heaven Website also contained over 20 images of hard-

---

[13] Presumably, the Operators of the Child Pornography Website had maintained records of e-mails used by child pornography purchasers on prior occasions, and chose these e-mails as an avenue to solicit new subscriptions.

[14] Upon further investigation, ICE agents determined this URL to be one of the Child Pornography Advertising Websites listed in footnote 5, supra.

[15] Based upon my experience investigating child pornography on the Internet and my conversations with other law enforcement officers, I have come to learn that the phrase "PTHC" is an acronym of "Pre-Teen Hard Core."

core child pornography.

38. The Pedo Heaven Website also contained a "join page" that, like the "join page" of the Child Pornography Advertising Website through which ICE agents had purchased a subscription in October 2005, contained fields for a purchaser to enter personal and credit card information in order to obtain access to the advertised images and videos of child pornography. Those fields required, among other information, the purchaser's first and last name, billing address, e-mail address, and credit card number, cvv, and expiration date. There was also a field for the purchaser to enter a proposed login and password. At the bottom of that webpage was a link titled "Submit."

39. On or about March 25, 2008, an ICE agent acting in an undercover capacity ("UC-2"), entered information into all of the fields on the "join page" of the Pedo Heaven Website using an undercover identity, including an undercover e-mail address ("UC-2 E-mail Account") and undercover credit card information. After completing all of the fields and clicking on the "Submit" link, another webpage appeared which displayed the following:

> Thank you for your Purchase!
>
> Credit Cards are verified and processed manually.
>
> Please wait up to 24 hours.
>
> You will receive all information in your e

mail.

If you will not receive e mail in 24 hours, this means that your card was declined

If you have any questions, e mail us nolimitzory@aim.com

Dear customers!

PLEASE ALL CONTACTS ONLY VIA THIS EMAIL!!! nolimitzory@aim.com

DO NOT SEND EMAILS TO ANY OTHER ADDRESSES Note: Never mention ABOUT SITE ACCESS OR MEMBERSHIP IN EMAILS. IF YOU HAVE ANY TROUBLES JUST EMAIL LIKE THAT:

"I still didn't get my purchase, please check it up"

40. On or about March 26, 2008, an e-mail from the e-mail address signamer@hotmail.com with the subject line "***Login Information***" was received at the UC-2 E-mail Account. The e-mail contained the login and password that UC-2 had entered on the "join page" of the Pedo Heaven Website on or about March 25, 2008, and included instructions to visit the Child Pornography Website. The e-mail message also stated that UC-2's undercover credit card would be charged by NEWSAC for the purchase price of $79.99. The e-mail further stated:

If you will receive email or phone call from anybody requesting about this transactions, just answer you purchased anti spyware software.

Note: Please don't share your password to other people. In case our password

> protection system detect multi usage, your password will be removed immediately without any notice. If you unhappy with our members area, you can send us refund request with description of reasons. And if we can't you satisfy, we shall make to you refund. Thank you!"[16]

41. On or about March 26, 2008, UC-2 accessed the Child Pornography Website. UC-2 was then transferred to a webpage that contained a login and password field. After entering the login and password contained in the e-mail from signamer@hotmail.com described in the previous paragraph, UC-2 was redirected to a webpage that made available thousands of images and videos of child pornography.

42. Among the images and videos UC-2 was able to access through that Child Pornography Website were the following:

a. An image with the file name of 66.232.124.43/444/pics/asia283.jpg depicting a prepubescent female engaged in sexual activity with an adult male. The image is taken from a frontal viewpoint. The prepubescent female is visible from her chin to her feet and is wearing pink and white "Barbie" sneakers and white underwear. The right hand of the adult male is visible. The prepubescent female is lying on her back on a flat surface, her legs are bent up at the knees and her feet placed flat on the surface she is lying on. Her wrists are bound to her calves with gray tape. The white underwear she is wearing has been partially ripped to expose her genital and anal regions. A green, cylindrical object is inserted into the anus of

[16] All misspellings and grammatical errors contained within the block quote are the errors of the original authors.

the prepubescent female by the adult male.

b. An image with the file name of 66.232.124.43/444/pics2/brasil023.jpg depicting a prepubescent female engaged in sexual activity with an adult male. The image is taken from a side viewpoint. The prepubescent female is visible from her head to her knees. She is fully nude. The adult male is visible from his neck to his calf area. He is fully nude. Also visible to left side of the prepubescent female is a third individual that appears to be another prepubescent female, visible from the chin down, she is fully nude, her partially developed breasts are visible, and in her right hand is a dark colored, elongated object. Off to the right side of the adult male appears to be a fourth individual whose right leg and hands are visible. This individual is holding a green colored lamp which is pointed toward the direction of the adult male and the prepubescent female. The prepubescent female is on her hands and knees on what appears to be a bed, her face is looking to her right, her legs are slightly parted. The adult male is kneeling on the bed behind the prepubescent female, his left hand is placed on the left hip of the prepubescent female and his right arm is extended back behind him. The erect penis is placed between the parted legs of the prepubescent female, and he is leaning back slightly.

c. A video with the file name 007-R@ygold-Lgassmania-6yo.mpg that is approximately 7 minutes and 32 seconds in length. The video depicts a prepubescent female engaged in sexual activity. During the video, her genital and buttock regions are visible, and she touches and fondles her genitals. At 4 minutes 50 seconds into the video, the prepubescent female lies on her back, brings her knees to her chest and inserts a long, cylindrical object into her anus, which appears to be a candlestick. This activity continues for the remainder of the video.

43. When the credit card statement for the undercover credit card used for the March 25, 2008 purchase made through the Pedo Heaven Website was received, it reflected a charge of $79.99 to NEWSAC.[17]

3. Search Warrants of the Server Hosting the Child Pornography

44. Through the use of commercially available search tools, ICE agents were able to determine that the images and videos of child pornography accessible through the Child Pornography Website described in the above paragraphs were contained on a computer server hosted by Hivelocity Ventures Inc., Sago Internet Park, Suite 303, 4465 West Gandy Boulevard, Tampa, Florida 33611 ("Hivelocity").[18]

45. Searches of the Hivelocity server that hosted the content available through the Child Pornography Website were performed on or about May 8, 2008 and July 11, 2008 pursuant to court-authorized search warrants. A review of the contents of the server revealed the presence of thousands of images and

---

[17] One of the e-mails from the Operators of the Child Pornography Website to the CW E-mail Account containing a list of subscribers included the information entered by UC-2 through the "join page" of the Pedo Heaven Website on or about March 25, 2008.

[18] There is no evidence to suggest that the owners of the servers at Hivelocity Ventures, Inc. had any knowledge that their server space was being used to host child pornography.

videos of child pornography. The contents were consistent with the material to which UC-2 had obtained access via the undercover subscription obtained in late March 2008. In addition, log files were obtained pursuant to the warrant. Those files contained a variety of data pertaining to individuals who had accessed the Child Pornography Website between in or about October 2007 through in or about June 2008, including e-mail addresses, subscriber IDs and IP addresses. ICE agents were able to cross-reference this data - particularly the e-mail addresses - with the lists of subscribers received at the CW E-mail Account to match log files with specific subscribers. ICE agents were thus able to determine which specific images were accessed by hundreds of individual subscribers and the time of such access.

4. **Searches of Servers Containing Signamer@hotmail.com and Nolimitzory@aim.com E-mail Accounts**

46. Through further investigation, ICE agents learned that the server that hosts the signamer@hotmail.com e-mail address - the e-mail address from which UC-2 received the March 26, 2008 e-mail described above - is owned by an entity named MSN Hotmail, 1065 La Avenida, Building No. 4, Mountain View, California 94043.

47. A search of the server that hosted the signamer@hotmail.com e-mail account was performed on or about

May 8, 2008 pursuant to a court-authorized search warrant. A second such search warrant was executed on this e-mail account on or about July 11, 2008. The information obtained pursuant to those warrants included stored electronic communications and other files reflecting communications to or from the signamer@hotmail.com e-mail account. Among the materials were e-mails relating to child pornography subscriptions like the one received at the ICE Undercover E-mail Account on or about March 26, 2008. In addition, numerous e-mails were recovered regarding requests, complaints and comments made by subscribers.

48. Through further investigation, ICE agents learned that the server that hosts the nolimitzory@aim.com e-mail address - the e-mail address from which the CW received subscribers' personal and credit card information as described above - was owned by AOL LLC, 22000 AOL Way, Dulles, Virginia, 21066.

49. A search of the server that hosted the nolimitzory@aim.com e-mail account was performed on or about May 16, 2008 pursuant to a court-authorized search warrant. The information obtained pursuant to that warrant included stored electronic communications and other files reflecting communications to or from nolimitzory@aim.com. Among the materials were e-mails from and to individuals who had purchased child pornography subscriptions, including e-mails from

individuals seeking refunds of their purchases of access to the images and videos of child pornography.

VII. PROBABLE CAUSE TO SEARCH THE SUBJECT PREMISES

A. Adrian CAZACU, at the "SUBJECT PREMISES" Purchased a Membership to the Child Pornography Website and Used the Membership to Access Child Pornography.

50. During the investigation described above, ICE agents learned that an individual named Adrian CAZACU who currently resides at the "SUBJECT PREMISES," purchased a membership to the Child Pornography Website. Furthermore, as described in detail below, that account was used to access child pornography images and videos.

51. On or about May 18, 2008, an e-mail from the Operators of the Child Pornography Website via nolimitzory@aim.com was received at the CW E-mail Account. That e-mail included a file containing the following information, among other things, that an individual had entered into the "join page" "http://vanyqit.com/private/joinc.html," one of the Child Pornography Advertising Websites, on or about May 20, 2008, for the purchase of access to the Child Pornography Website.

a. Name: Adrian CAZACU

b. E-mail Address: therockcafede@yahoo.com

c. Billing address: 2704 W. Ball Rd. 1C, Anaheim, CA

92804

d. Telephone number: 714-499-2867

e. Credit Card Number: [redacted] 7139

f. Proposed login: transrock

g. Proposed password: eu6sase

The data also contained the IP address, 69.226.57.194 that was captured when Adrian CAZACU submitted the information requested on the "join page" as listed above.

52. On or about May 18, 2008, an e-mail was sent from the CW E-mail Account to the Operators of the Child Pornography Website indicating that the credit card number submitted by Adrian CAZACU had been successfully processed. Thereafter, the Operators of the Child Pornography Website determined whether to grant Adrian CAZACU access to the Child Pornography Website.

53. On or about March 27, 2009, I reviewed the content of the Child Pornography Website, and the related advertising pages, obtained from the search warrants executed on Hivelocity and found the site to contain exclusively child pornography and child erotica. In addition to child pornography images and videos, the Child Pornography Website's log files were recovered and were found to contain the dates and times that a user account, and its IP Address, accessed the various child pornography images and videos available on the Child Pornography

Website.

54. On March 27, 2009, I reviewed the advertising page providing hyperlink to the URL for "join page," "http://vanyqit.com/private/joinc.html,". The advertising page, located at http://vanyqit.com/private/joinc.html, contains a graphic in the top left corner of the page that states the following:

PEDO HEAVEN
Simply the best
PTHC place in the
entire WORLD!

The rest of the advertising page is scattered with images of child pornography. One of the images displayed on the page is of a nude female child appearing to be under the age of 12 years old on top of a bed on her hands and knees. Directly behind child is a nude male adult who is grabbing the child's hip with his left hand and appears to be penetrating, or at least touching, the female child's vagina with his penis. Towards the bottom of the advertising webpage there is a "sample section" containing in excess of 15 different child pornography images. Just above and below these "samples" are text hyperlinks that state: "CLICK HERE TO JOIN."

55. On or about June 23, 2009, I reviewed the log files obtained as a result of the search warrants executed on the server hosted by Hivelocity. I found that on May 20, 25, 26, 29, 30, 31, June 1 and 5 2008, CAZACU's account,

"therockcafede@yahoo.com," was used to access and view numerous images and videos of child pornography made available on the Child Pornography Website.

56. On or about March 27, 2009, I viewed three (3) of the images/videos depicting what appears to be child pornography accessed by CAZACU's account, "therockcafede@yahoo.com." These images are described below in sub-paragraphs a, b, and c:

a. A video file titled "Pthc - Family Fun Pedo 2 8yo Boys Little (Mom Sex Kiddies.mpeg": This video was accessed by an individual controlling username "therockcafede@yahoo.com," on May 26, 2008. The video is approximately one (1) minute and thirty (30) seconds long. It depicts what appears to be an adult nude female lying on her back with her legs raised in the air, and what appears to be a prepubescent nude male child with an erect penis facing away from the camera, standing between the legs of the adult female. The adult female has both her hands pressed-up on the buttocks of the male child, it appears that the child is penetrating the vagina of the adult female. The video also depicts another prepubescent nude male child lying next to the nude adult female, as the adult female rubs the erect penis of the male child. In other parts of the video the adult female and one of the boys appear to be in tandem oral-copulating what appears to be an adult male.

An adult male who is nude and lying down on his back is masturbating as the two prepubescent boys alternate urinating on the adult males erect penis.

b. An image file titled "brasil035.jpg": This image was accessed by an individual controlling username "therockcafede@yahoo.com," on May 30, 2008. The image depicts what appears to be a prepubescent female child who is nude and appears to be under the age of 6 years old. She appears to be sitting on a bed, looking directly into the camera. The prepubescent child is using her right hand to hold her right leg in the air, clearly displaying her vagina. There is a black elongated object, appearing to be a vibrator, lying on the bed within inches of the child's open legs.

c. An image file titled "asia012.jpg": This image was accessed by an individual controlling username therockcafede@yahoo.com, on May 31, 2008. The image depicts what appears to be a prepubescent female child wearing a blue jean jack, lying on her back with her legs spread open. The prepubescent child appears to have her arms wrapped around the torso of what appears to be an adult male who is nude and is lying on top of the child. The face of the nude adult male has been digitally blocked with a white box. The nude adult male appears to have placed his genitals on top of, or in the child's

vagina. Another female child can be seen behind the male adult lying on her stomach with her arm extended and appears to be touching the genitals of the adult male from behind.

B. **Identification of CAZACU and the "SUBJECT PREMISES"**

57. ICE agents determined that an individual named Adrian CAZACU, who previously resided at 2704 W. Ball Rd. 1C, Anaheim, CA 92804, has since relocated his residence to 3416 W. Orange Ave. Apt #205W, Anaheim, CA 92804, current "SUBJECT PREMISES." Based on my training and experience, individuals who receive and attempt to receive child pornography often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location for many years. For the reasons set forth, there is probable cause to believe that evidence of the receipt and possession of child pornography will be located at the current "SUBJECT PREMISES."

58. On or about January 12, 2009, ICE agent's subpoenaed records for credit card purchases made using credit card number XXXXXXXXXXX7139. The subpoenaed account confirmed that the credit card was issued from Bank of America to Adrian CAZACU at 2704 W. Ball Rd. Apt 1C. These records also revealed that on

May 21, 2008, a charge in the amount of $79.99 for NEWSAC was billed to that credit card account.[19]

Based on my training and experience and that of other agents, individuals who make a purchase into a website with child pornographic content often contest or reverse the related credit card charges in an effort to disassociate themselves from the website and/or note their own error in making the purchase. On an unknown date in January 2009, my review of the aforementioned credit card/debit bank records for the periods April 2008 through March 2009, of Adrian CAZACU, Bank of America noted no contested or reversed charges for the purchase of one subscription into the illegal Child Pornography Website.

59. On an unknown date in September 2008, and again in May 2009, summons were issued to Yahoo! Inc. for IP logs for email address "therockcafede@yahoo.com." Representatives of Yahoo! Inc. confirmed that the e-mail address, "therockcafede@yahoo.com.", is registered to Mis. Alina Krieger (wife of Adrian CAZACU) with the address listed as 2704 w. Ball Rd., Anaheim CA 92804, and is still in use after the move to the current "SUBJECT PREMISES."

60. or about June 11, 2009, record checks with law

---

[19] A very small percentage of the subscribers were charged $75.95.

enforcement indices revealed that an individual named Adrian CAZACU with a date of birth of September 19, 1965, resides at the "SUBJECT PREMISES."

62. On July 7, 2009, at approximately 1510, SA Monica Abend and SA Troy Kennedy of the Orange County ICE Office went to the "SUBJECT PREMISES" as a ruse. A white female answered the door and provided the following information:

a. The white female told agents that her name was Alina Krieger and that she has been living at the "SUBJECT PREMISES" since March 26, 2009, as the Apartment Manager with husband Adrian CAZACU and fourteen (14) year old daughter.

b. The individual who identified herself as Alina Krieger told agents that no one else lives at the "SUBJECT PREMISES."

c. During the ruse SA Abend noticed what appeared to be a computer in use, resting on a desk, facing southwest in the front room of the "SUBJECT PREMISES."

C. **Individuals Who Exhibit An Interest In Child Pornography**

63. There is probable cause to believe that Adrian CAZACU has received or attempted to receive child pornography. First, as detailed above, in May 2008, CAZACU spent $79.95 to purchase a membership to the Child Pornography Website. Child pornography is clearly illegal, yet CAZACU so desired access to this

material that he engaged in the high-risk behavior of giving his name, email address, credit card information and address. Furthermore, log files show that he used the membership to access child pornography on multiple occasions.

64. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals, like CAZACU, who are involved in the receipt and attempt to receive child pornography:

a. Those who receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who receive and attempt to receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions

of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who receive and attempt to receive child pornography often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, those who receive and attempt to receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the individual to view the collection, which is valued highly.

e. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such

correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Those who receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

D. **Evidence Will be Found at the "SUBJECT PREMISES"**

65. Even if CAZACU used a computer located elsewhere to access illegal child pornography, it is more likely than not that evidence of this access will be found in his home. Child pornography received via computer is extremely mobile. Through computer technology, digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto thumb drives so small they fit onto a keychain. Just as easily, these files can be copied onto floppy disks or compact disks, stored on I-Pods, Blackberries, and cellular telephones. Because CAZACU likely collects and values child pornography, which is easily-stored and duplicated, there is probable cause to believe that evidence of CAZACU's child pornography collection will be

found in the "SUBJECT PREMISES."

E. **Computer Forensics Allows Recovery of Evidence, Even After Deletion**

66. Based on my training and experience, as well as my conversations with digital forensics agents, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a

temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

VII. DIGITAL DATA

67. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search digital devices for data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and

specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, software application or operating system that is being searched.

b. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Digital devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since digital data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the digital devices from which the data will be extracted.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable

of storing 500 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 240 million pages of data, that, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 GB drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to